



UNITED FARMERS TELEPHONE COMPANY

216 North Main • Everly, Iowa 51338 • Phone 712-834-2211

February 28, 2008

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C. 20554

Received & Inspected

MAR 03 2008

FCC Mail Room

RE: EB Docket No. 06-36
Annual CPNI Certification for Year 2007

Dear Ms. Dortch:

In accordance with Public Notice DA 08-171, issued on January 29, 2008, attached is the annual CPNI certification filing for the year of 2007 for United Farmers Telephone.

Sincerely,

Roxanne White
General Manager

Attachment

cc: Federal Communications Commission (*two copies*)
Enforcement Bureau
Telecommunications Consumers Division
445 12th Street, SW
Washington, D.C. 20554

Best Copy and Printing, Inc. (*one copy*)
445 12th Street
Suite CY-B402
Washington, D.C. 20554

No. of Copies rec'd 0
List ABCDE

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 28, 2008

Name of company covered by this certification: United Farmers Telephone Co.

Form 499 Filer ID: 801885

Name of signatory: Roxanne White

Title of signatory: General Manager

I, Roxanne White, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

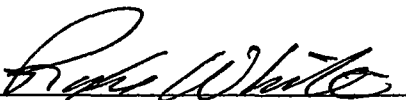
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

If affirmative: NA

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

If affirmative:

Signed 

ATTACHMENT

OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

United Farmers Telephone has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training:

The Compliance Officer arranges for the training of all employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. **Each employee knows where the CPNI Manual is located with all of the rules and regulations, and is easily accessible to all employees.**

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all employees.

A copy of the Company's disciplinary process is kept in the **Company Manual**.

Customer Notification and Request for Approval to Use CPNI

The Company has provided notification to its customers of their CPNI rights. A copy of the notification is also provided to all new customers that sign up for service.

The company's position is that all customers have opted-out, unless we exercise a one-time use of opting-in from a verbal authorization from the customer to be solicited for other company services.

The company's position is that all customers are opting out, unless at time of install or service an employee may ask if they would like to hear about any other services offered by our company, which is giving the customer the opportunity to opt in or out at that time. Thereafter, the one-time opting in, the customer's status will change back to opted-out until future verbal authorization from the customer.

SAMPLE

Marketing Campaigns

The Company does not use CPNI for marketing purposes.

Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

In-office visit - the customer must provide a valid photo ID matching the customer's account information.

Customer-initiated call – the customer is authenticated by providing the last four digits of their social security number as the answer to their question and must be listed as a contact on the account.

If the customer wants to discuss call detail the following guidelines are followed:

- Provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.
- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Address of record
- Account status
- Authorized users

The notification to the customer will be made by a Company-originated written notification to the customer's address of record. The company's billing software generates a letter based on the above account changes.

Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.
- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

SAMPLE

- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.
- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.
- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

Record Retention

The Company retains all information regarding CPNI. General CPNI information is located in our CPNI Manual, and personal information concerning accounts is in a separate file in our billing department. Below is a listing of our record retention guidelines:

- CPNI notification and records of approval – two years
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years

Miscellaneous

Nothing that is not listed above.

APPENDIX 3

Annual 47 C.F. R. § 64.2009(e) CPNI Certification

EB Docket No. 06-36

Annual 64.209(e) CPNI Certification for: 2007

Date Filed: February 11, 2008

Name of Company covered by this certification: The City of San Bruno, d/b/a
San Bruno Municipal Cable TV

Form 499 Filer ID: 826834

Name of signatory: Constance Jackson

Title of signatory: City Manager

I, Constance Jackson, certify that I am City Manager of the City of San Bruno, and acting as an agent of City of San Bruno, that I have personal knowledge that the City of San Bruno has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.

Attached to this certification is an accompanying statement explaining how the City of San Bruno's procedures ensure that the City of San Bruno is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The City of San Bruno has not taken any actions against data brokers in 2007.

The City of San Bruno has not received any customer complaints in 2007 concerning the unauthorized release of CPNI.

Signed: Constance Jackson

ATTACHMENT TO OFFICER'S CPNI COMPLIANCE CERTIFICATE

Statement Regarding CPNI Operating Procedures

The City's written CPNI Operating Procedures ensure that the City will be in compliance with 47 U.S.C. § 222 and the rules contained in the Title 47, Chapter 1, Subchapter B, Part 64, Subpart U of the Code of Federal Regulations. Included among the provisions of the City's CPNI Operating Procedures are:

- A requirement that the City have at all times a CPNI Compliance Supervisor to supervise the implementation of the City's CPNI Operating Procedures.
- Detailed procedures for safeguarding CPNI, including procedures for customer authentication and password protection of CPNI.
- Detailed procedures for determining what type of customer approval is necessary for use, disclosure and access to CPNI.
- Detailed procedures for obtaining opt-out and opt-in approval from customers.
- A requirement that the billing system records for customers' accounts allow the status of the customer's CPNI approval to be easily ascertained.
- A requirement for supervisory approval of all outbound marketing campaigns, including determination of any customer approval requirements for the campaigns.
- A requirement that personnel be trained as to when they are and are not authorized to use CPNI.
- A written disciplinary process for misuse of CPNI.
- Detailed filing, notice and recordkeeping requirements.
- Detailed procedures to be followed in the event of a breach of CPNI.

APPENDIX 3

Annual 47 C.F. R. § 64.209(e) CPNI Certification

EB Docket No. 06-36

Received & Inspected

MAR 03 2008

FCC Mail Room

Annual 64.209(e) CPNI Certification for: 2007

Date Filed: February 11, 2008

Name of Company covered by this certification: The City of San Bruno, d/b/a San Bruno Municipal Cable TV

Form 499 Filer ID: 826834

Name of signatory: Constance Jackson

Title of signatory: City Manager

I, Constance Jackson, certify that I am City Manager of the City of San Bruno, and acting as an agent of City of San Bruno, that I have personal knowledge that the City of San Bruno has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.

Attached to this certification is an accompanying statement explaining how the City of San Bruno's procedures ensure that the City of San Bruno is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The City of San Bruno has not taken any actions against data brokers in 2007.

The City of San Bruno has not received any customer complaints in 2007 concerning the unauthorized release of CPNI.

Signed: Constance Jackson

No. of Copies rec'd 0+1
List ABCDE

ATTACHMENT TO OFFICER'S CPNI COMPLIANCE CERTIFICATE

Statement Regarding CPNI Operating Procedures

The City's written CPNI Operating Procedures ensure that the City will be in compliance with 47 U.S.C. § 222 and the rules contained in the Title 47, Chapter 1, Subchapter B, Part 64, Subpart U of the Code of Federal Regulations. Included among the provisions of the City's CPNI Operating Procedures are:

- A requirement that the City have at all times a CPNI Compliance Supervisor to supervise the implementation of the City's CPNI Operating Procedures.
- Detailed procedures for safeguarding CPNI, including procedures for customer authentication and password protection of CPNI.
- Detailed procedures for determining what type of customer approval is necessary for use, disclosure and access to CPNI.
- Detailed procedures for obtaining opt-out and opt-in approval from customers.
- A requirement that the billing system records for customers' accounts allow the status of the customer's CPNI approval to be easily ascertained.
- A requirement for supervisory approval of all outbound marketing campaigns, including determination of any customer approval requirements for the campaigns.
- A requirement that personnel be trained as to when they are and are not authorized to use CPNI.
- A written disciplinary process for misuse of CPNI.
- Detailed filing, notice and recordkeeping requirements.
- Detailed procedures to be followed in the event of a breach of CPNI.

Annual 47 C.F.R. 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date Filed: February 27, 2008

Name of company covered by this certification: e-Tel Murray, LLC

Form 499 Filer ID: 821714

Name of signatory: Renee Hayden

Title of Signatory: Chief Operating Officer

Received & Inspected

MAR 03 2008

FCC Mail Room

I have personal knowledge that e-Tel Murray, LLC (and its affiliates) established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules and requirements in Subpart U of part 64 of the Federal Communications Commission's Rules (47 C.F.R. 64.2001 thru 64.2011). The attached Statement of CPNI compliance explains how the Company's operating procedures ensure that it is in compliance with the foregoing FCC rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signature

Renee Hayden

Printed Name

Renee Hayden

Date

2.26.08

No. of Copies rec'd
List ABCDE

048

**CERTIFICATE OF COMPLIANCE WITH PROTECTION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION RULES**

Renee Hayden signs this Certificate of Compliance in accordance with Section 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and the FCC's Code of the Federal Regulations (CFR) Title 47 64.2009, on behalf of R. Tel Murray, LLC. This Certificate of compliance addresses the requirement of FCC's (CFR) Title 47 64.2009 that the Company provide both a Certificate of compliance and a "statement accompanying the certificate" to explain how its operating procedures ensure compliance with the FCC's (CFR) Title 47 64.2001-2011.

On behalf of the company, I certify as follows:

1. I am the Chief Operating Officer of the Company. My business address is 601 Broadway, Paducah KY 42001.
2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to customer proprietary network information (CPNI).
3. The company has established a system by which the status of a customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of the applicable law has occurred.
4. The Company trains its personnel regarding when they are authorized to use CPNI, as well as when they are not authorized to use CPNI. However, Company personnel make no decisions regarding CPNI without first consulting with myself or other supervisors. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.
5. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.
6. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

**CERTIFICATE OF COMPLIANCE WITH PROTECTION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION RULES (Cont'd)**

7. The Company's policy is to maintain records of a CPNI breach for a minimum of two years. These records will include a description of the steps the company took to prevent the breach, how the breach occurred, the impact of the breach and proof of notification to law enforcement and the customer, if applicable.
8. The Company has a supervisory review process regarding compliance with the FCC's rules relating to protection of CPNI for outbound marketing situations. The purpose of this supervisory review process is to ensure compliance with all rules prior to using CPNI for a purpose for which customer approval is required. Company personnel, prior to making any use of CPNI, must first consult with myself or another supervisor regarding the lawfulness of using the CPNI is proper, either a supervisor or I consult one or more of the following: the Company's own compliance manual, the applicable FCC regulations, the FCC's Compliance Guide, and if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval from either a supervisor or I regarding any proposed use of CPNI.
9. Further, both a supervisor and I personally oversee the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. I also review all notices required by the FCC regulations for compliance therewith.
10. A supervisor and I also ensure that the Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI.
11. Both a supervisor and I personally oversee completing and submitting EB Docket No. 06-36, which is due on or before March 1 each year. The form includes explanation of any action taken against data brokers, a summary of all customer complaints, and an explanation of breaches, if applicable.

Signature Bernie Hayden
Company e-Tel Murray, LLC
Date 2.26.08